State Laboratory Institute
~
System Policies and Procedures

Created by Sean F. Fiandaca Created on 5/4/2004 10:41:00 AM
Last saved by Sean F. Fiandaca policy_rev_2.doc Updated on 2/2/2005 7:19 AM

DPH Backup Process

Daily Backup Routine

The following procedure describes how a backup administrator should maintain the current backup strategy. Described herein is the daily process of logging and monitoring the established backup jobs.

1) Log on to MSLNT-BU-01
2) Start Backup Exec.
3) Within Backup Executive go to the 'Job Monitor' tab (see illustration A).
4) Sort page by Start Time in descending order.
5) The first items (in blue) are jobs scheduled for later. Underneath these you will find the most recently completed jobs.
6) The Monthly (Daily) Jobs are as follows:
7) CoreFullINH (CoreIncINH)—a backup of the Domain Controllers and the Remote Access server.
8) DevelopmentFullINH (DevelopmentIncINH)—a backup of the development Web servers.
9) MiscFullOSB (MiscIncINH)—Drugs, LRN, VCMS, and EIS.
10) SharedFullOSB (SharedIncOSB)—Backs up shared files on MSL1 and MSL2.
11) DatabaseArcOSB—Run weekly, backups and archives the SQL database dumps.
12) PrivateFullINH (PrivateIncINH)—Backs up private folders on MSL1.

Note: In this naming convention, any job with DIFF is a Differential Backup, INC is an Incremental Backup, FULL is a Full Backup, OSB is an Off-Site Backup, and Inhouse is the On-Site set.

13) Fill out Backup Job Checklist, located at \\mslisnt\Utilities\BackupDocs, (see illustration B and C, *note B is for days Monday through Friday and C is for Saturdays and Sundays*) by checking the following items:
    a) Check the job completion status in the column labeled 'Job Status'.
    b) Double click on each job from this morning to view the properties (see illustration D).
    c) Within properties window, select the Log File tab.
    d) Should a job fail, print out this log and note the document name on the checklist. Include the document in the 'Error Logs' section in the 'Backup Job Checklist Archive' Binder.
    e) Scroll down on the middle window about 2 lines and record the Media Cartridge Label in the 'Tape' column on the Backup Job Checklist (highlighted in blue on illustration E).
    f) Record any notes you need for this job.
    g) If checking on Monday, please repeat process for prior Sunday. Sunday jobs will differ based on the week of the month, please fill in the appropriate section on the Sunday Checklist (see illustration C), and see 'Saturday and Sunday Backup Routine' for additional instructions.
    h) Depending on which jobs failed you may be required to notify a person or department of the problem. See the 'Call List'.
14) At the end of the week remove any tapes which are full and archive them. You can tell that a tape is full by looking at what tapes were being used by the job at the beginning of the week as opposed to which tape is used at the end of the week. For instance, if on Monday the CoreIncINH job was using tape msl100045, and on Friday it used tape msl100056, then you know that tape msl100045 is full. Any tape from an OSB job should be set aside until the end of the month when it will be removed from these premises and archived.
15) Refill changer with blank tapes.

Saturday and Sunday Backup Routine

The Saturday and Sunday Procedures differ from the Daily Backup Procedure in that full backups are done instead of differential and incremental backups, these are done on the first and third Saturday and first Sunday of each month.

These additional jobs should be self explanatory if you apply the same naming convention logic as presented in the Daily Backup Routine. For instance, the CoreIncInh job is the same as the CoreFullINH job, excepting that the latter is a full job instead of an incremental backup.

Important: The Friday before the first Saturday or first Sunday of the month, (which ever comes first) all used and partially used tapes should be removed from the changer and replaced with blank media. If these tapes are from OSB jobs they should be sent to the Off-Site archive facility, include with these tapes a copy of the 'Daily Backup Job Checklist' for the month at hand. Other tapes (Inhouse) should be saved for three months and then recycled.

Off-Site Backup Information

At the beginning of each month we send to the Worcester facility our Off-Site backup set from the month prior to the one just ending, and we place the archive set from the most recent month to be stored in a separate building on campus. The off-site set is kept indefinitely in a safe environment as an archive of the state of our servers at any given time. These tapes will contain sufficient information to restore any mission critical information to any specific day as far back as the archive goes.

Should one of these tapes be required, first look in the 'Backup Job Checklist Archive Binder' to find out which tapes you are interested in, and then send to Worcester a runner to pick up those tapes. Because of the length of time required to go back and forth with these tapes, it is better to request extra tapes to be certain you will get the information required. After use, the tapes should be returned to Worcester.

DPH Restore Process

The following describes the basic process of recovering lost files. This is not a disaster recovery solution; rather a method of restoring lost user files.

1) Log on to MSLNT-BU-01
2) Start Backup Exec.
3) Within Backup Executive go to the 'Restore Selections' tab (see illustration F).
4) From the View Menu select 'Show Restore Selections by Volume'.
5) In the left-hand window expand the server which housed the information you would like to restore.
6) Expand the volume or container where the file is located.
7) Expand the date from which you want the restore to come. If the date you want to restore from is too far past, you will need to go to the manual logs in the folder 'Backup Job Check List' located in the server room and find out which tape the job was recorded on. Refer to the Daily Backup Routine section of this document section 6 and 7 to find out what backup job the file would have been contained in and how it would have been entered into the records. When you find the tape, insert it into the changer and run catalog on it from the 'Device Management' section. After doing so restart this step, you should now find the date you were looking for.
8) Drill down in the left-hand window until you find the file or folder, which you want to restore, and check if off (see illustration G, in which the MSL1\Vol1\Apps\bcs\app folder from 11/15/00 has been selected). If you do not find the file you are looking for it may be necessary to use a different date, in which case return to step 7.
9) Take note of the name of the tape which you are selecting, it is listed after the date in selection step 7 and before the word 'Set', it will be something similar to 'msl100054'.
10) When all selections have been made, click the 'Restore' button.
11) You will be presented with the restore dialog box (see illustration H), enter the following information:
    a) Job Name: select a name, which you will be able to remember and which is descriptive of the job.
    b) On the Advanced Tab (see illustration I) in the 'Restoring Existing Files' area, select the option which is appropriate for you (Restore over existing files/ Skip if file exists/ Skip if existing file is

more recent). If you are unsure then be certain to redirect the files to a different folder (described in subsection c below).

c) Redirection: use this option to restore the file to a location other than where it originally came from. This option is recommended if you are at all unsure of whether or not to replace the other files which may be in the folder you are restoring.

d) Select 'Save Job', dialog box will close.

12) Fill out the File Restore Checklist.dot completely and submit it to the designated supervisor for
    a) approval, it is located in the F:\SHARED\Information_Services\Change Control directory
13) Once it is approved, go to 'Job Definitions' tab, and find the job which you just created.
14) If you are ready to run the job, right click on it and select 'Run Now'. You can monitor the job's progress from the 'Job Monitor' tab.
15) Once completed, fill out the remainder of the File Restore Checklist and submit it for archiving.

UMass Backup Plan

Daily Backup Routine

The following procedure describes how a backup administrator should maintain the current backup strategy. Described herein is the daily process of logging and monitoring the established backup jobs.

1) Log on to EDJPBU01
2) Start Backup Exec.
3) Within Backup Executive go to the 'Job Monitor' tab (see illustration A).
4) Sort page by Start Time in descending order.
5) The first items (in blue) are jobs scheduled for later. Underneath these you will find the most recently completed jobs.
6) The Daily Incremental Jobs are as follows:
7) PrivateIncINH—a backup of the private directories on EDJPFP02.
8) SharedIncOSB—a backup of the remaining directories on file server EDJPFP02.
9) BioServersIncOSB—a backup of Biologics EDJPAPP02, EDJPAPP03 and EDJPWEB03.
10) CoreIncINH—a backup of Development Database and Web servers.
11) ExchangeIncOSB—a backup of Exchange servers.

Note: In this naming convention, any job with INC is an Incremental Backup, FULL is a Full Backup, OSB is an Off-Site Backup, and INH is the On-Site set.

12) Fill out Backup Job Checklist, located in the server room, (see illustration J and K, *note J is for days Monday through Saturday, and K is for Sundays*) by checking the following items:
    a) Check the job completion status in the column labeled 'Job Status'.
    b) Double click on each job from this morning to view the properties (see illustration D).
    c) Within properties window, select the Log File tab.
    d) Should a job fail, print out this log and note the document name on the checklist. Include the document in the 'Error Logs' section on the 'Backup Job Checklist Archive' Binder.
    e) Scroll down on the middle window about 2 lines and record the Media Cartridge Label in the 'Tape' column on the Backup Job Checklist (highlighted in blue on illustration E).
    f) Record any notes you need for this job.
    g) If checking on Monday, please repeat process for prior Sunday. Sunday jobs will differ based on the week of the month, please fill in to the appropriate section on the Sunday Checklist (see illustration C), and see 'Sunday Backup Routine' for additional instructions.
    h) Depending on which jobs failed you may be required to notify a person or department of the problem. See the 'Call List'.
13) At the end of the week remove any tapes which are full and archive them. You can tell that a tape is full by looking at what tapes were being used by the job at the beginning of the week as opposed to which tape is used at the end of the week. For instance, if on Monday the PrivateIncINH job was using tape UM0020, and on Friday it used tape UM0025, then you know that tape UM0020 is full. Any tape from an OSB job should be set aside until the end of the month when it will be removed from these premises and archived.
14) Refill changer with blank tapes.

Sunday Backup Routine

The Sunday Procedure differs from the Daily Backup Procedure in that full backups are done instead of differential and incremental backups, these are done on the first and third Sunday of each month.

These additional jobs should be self-explanatory if you apply the same naming convention logic as presented in the Daily Backup Routine. For instance, the SharedIncOSB job is the same as the SharedFullOSB job, except that the former is an incremental job instead of a full backup.

Important: The Friday before the first Sunday of the month, all used and partially used tapes should be removed from the changer and replaced with blank media. If these tapes are from OSB jobs they should be sent to the Off-Site archive facility, include with these tapes a copy of the 'Daily Backup Job Checklist' for the month at hand. Other tapes (Inhouse) should be saved for three months and then recycled.

Off-Site Backup Information

At the beginning of each month we send to the Worcester facility our Off-Site backup set from the month prior to the one just ending, and we place the archive set from the most recent month to be stored in a separate building on campus. The off-site set is kept indefinitely in a safe environment as an archive of the state of our servers at any given time. These tapes will contain sufficient information to restore any mission critical information to any specific day as far back as the archive goes.

Should one of these tapes be required, first look in the 'Backup Job Checklist Archive' Binder to find out which tapes you are interested in, and then send to Worcester a runner to pick up those tapes. Because of the length of time required to go back and forth with these tapes, it is better to request extra tapes to be certain you will get the information required. After use, the tapes should be returned to Worcester.

UMass Restore Process

The following describes the basic process of recovering lost files. This is not a disaster recovery solution; rather a method of restoring lost user files.

1) Log on to EDJPBU01
2) Start Backup Exec.
3) Within Backup Executive go to the 'Restore Selections' tab (see illustration F).
4) From the View Menu select 'Show Restore Selections by Volume'.
5) In the left-hand window expand the server which housed the information you would like to restore.
6) Expand the volume or container where the file is located.
7) Expand the date from which you want the restore to come. If the date you want to restore from is too far past, you will need to go to the manual logs in the folder 'Backup Job Check List' located in the server room and find out which tape the job was recorded on. Refer to the Daily Backup Routine section of this document section 6 and 7 to find out what backup job the file would have been contained in and how it would have been entered into the records. When you find the tape, insert it into the changer and run catalog on it from the 'Device Management' section. After doing so restart this step, you should now find the date you were looking for.
8) Scroll down in the left-hand window until you find the file or folder, which you want to restore, and check it off (see illustration G, in which the MSL1\Vol1\Apps\bcs\app folder from 11/15/00 has been selected). If you do not find the file you are looking for it may be necessary to use a different date, in which case return to step 7.
9) Take note of the name of the tape which you are selecting, it is listed after the date in selection step 7 and before the word 'Set', it will be something similar to 'UM0025'.
10) When all selections have been made, click the 'Restore' button.
11) You will be presented with the restore dialog box (see illustration H), enter the following information:
    a) Job Name: select a name, which you will be able to remember and which is descriptive of the job.
    b) On the Advanced Tab (see illustration I) in the Restoring Existing Files area, select the option which is appropriate for you (Restore over existing files/ Skip if file exists/ Skip if existing file is more recent). If you are unsure then be certain to redirect the files to a different folder (described in subsection c below).

c) Redirection: use this option to restore the file to a location other than where it originally came from. This option is recommended if you are at all unsure of whether or not to replace the other files which may be in the folder you are restoring.
d) Select 'Save Job', dialog box will close.

12) Fill out the File Restore Checklist.dot completely and submit it to the designated supervisor for
a) approval, it is located in the F:\SHARED\Information_Services\Change Control directory
13) Once it is approved, go to 'Job Definitions' tab, and find the job which you just created.
14) If you are ready to run the job, right click on it and select 'Run Now'. You can monitor the job's progress from the 'Job Monitor' tab.
15) Once completed, fill out the remainder of the File Restore Checklist and submit it for archiving.

Network Rights Assignment

Network rights assignment can be thought of in two sections, user rights and group rights. The latter being the preferred method of rights assignment because it is inherently easier to manage.

Group Creation and Rights

All group creation must be accompanied by a change control. The change control should stipulate the name of the group, what file rights the group has, who requested the creation of the group, and who was added to the group. Every group should have a responsible party, who can authorize additions to the group. The responsible party is typically the user who requested that the group be created, or the person now occupying the role of that person. This should be clearly documented in the change control.

User Creation and Rights

An Employee Access Request Form must accompany all new user request, termination requests, and user rights changes. The administrative process for this is as follows:

1) Request form is submitted in writing to front desk, a supervisor must sign this.
2) Depending on the department of the user, the appropriate check list is picked up from 102b (Sean's room).
3) The modification/addition/or deletion is done per the process on the checklist.
4) The end user, or their supervisor is informed of the completion of the task, and if necessary, an appointment is made to set up the user's workstation.
5) Check sheet is signed and stapled to the original form.
6) The forms are promptly filed in front filing cabinet, or in the case of BIO users, returned to the Biologics Computer Services Coordinator and a duplicate is filed.

Disaster Recovery

Disasters come in many shapes and sizes, and as such each type of disaster warrants a different response. What follows is a list of foreseeable disaster scenarios, and the response that we have prepared for each. The disasters are listed in approximate order of magnitude, as judged by down time, hardware cost and complexity of response.

Data Loss Due to User Error

In this scenario we would merely restore data from the most recent backup. Any work done since the most recent backup would be lost. The amount of data lost would depend on the length of time since the backup. Systems will be backed up at a minimum of once per night to tape, additionally databases can be backed transactionally more frequently then this (see Database Standards: Best Practices: Backup).

Power Loss

All production systems capable of redundant power will have redundant power supplies (DL360 do not have this capability), and be hooked up to battery backup devices. The building itself has generators in the event of system wide power failure.

Disk Failure

All disk subsystems will be designed with redundancy, so that no single disk failure will result in data loss. We will maintain a supply of disks, such that every disk type running at the facility will have an available replacement disk. Once the replacement disk is installed and the array controller has time to rebuild the array, then a state of fault tolerance will be returned. For high priority systems an on-line spare will be kept to further protect the server from failure.

Server Failure

A cold spare of each server type will be maintained at the facility. Should a server fail due to a hardware failure, the disk subsystem may be removed from the damaged server and swapped into the spare server. This will result in minimal down time as the new server is reconfigured with the disks from production.

Server Loss

Should a server be completely lost, the spare server with spare drives will have to be used. The most recent data backup will have to be restored to the system. Any data updated since the last backup will be lost. This will involve significant down time.

Loss of Network Infrastructure Device

We will maintain a duplicate of every switch within the building, so that should a switch fail we can replace that switch.

Total Loss

It is impossible given our current funding situation to maintain a completely redundant system. In the event of a complete loss of the servers, network, and/or the building, all we will have is the off-site backups of the data, which may be as much as two months old (see Off-Site Backup Information).

Preventive Maintenance

Anti-Virus

Norton Anti-Virus is used for an enterprise level anti-virus solution. Every night the NAV parent server checks the Symantec Website for newer virus definitions and then downloads them when available. The parent server then distributes them to all servers and clients. Symantec System Console is used to monitor the virus definition status. Each e-mail server also has a NAV client for exchange, which monitors incoming and outgoing e-mail for viruses. Any virus that is detected will be intercepted and an alert will be sent to the sender, the recipient, and the email administrators. Every three days the exchange server checks the Symantec Website for newer virus definitions and then downloads them when available.

Compaq Insight Manager

Compaq Insight Manager (CIM) is running on all severs to monitor server health. Should a statistic go into the unhealthy range, the CIM monitor server will send an alert to all Computer Services senior support staff. Biologics servers are configured to email the Biologics Computer Services Coordinator as well.

Periodically tests are performed to ensure that the product is functioning as it should.

Database Standards

Naming conventions

Database Name

The database name should be short and descriptive, and should not contain any special characters. Nor should the database name be the same as any other database (except in a production/test/development scenario) or network resource.

Table Name

All table names should be short and descriptive, and should not contain any special characters (this includes the underscore [_] character). The name should be prefixed by 'tbl' to indicate what type of object it is (for ease of reference in system table sysobjects).

Special Table Types

Linkage tables (tables which provide for a Many to Many relationship) should be named by the root name of each linked table in alphabetical order. For instance, if a many to many relationship between tblBoxes and tblCardboard exists, the linkage table should be named tblBoxesCardboard. Note: A table of this type should contain only 4 fields, the two foreign keys, a ID field and a GUID [if GUID is required].

View Name

View names should be short and descriptive, and should not contain any special characters. The name should be prefixes by 'v' to indicate what type of object it is. Whenever possible a diagram of the view should be prepared.

Stored Procedure Name

All stored procedure names should be short and descriptive, and should not contain any special characters. The name should be prefixes by 'sp' to indicate what type of object it is. Do not use 'sp_' as this suffix has special meaning in SQL 2000 and may produce unexpected results.

Primary key

The primary key field name should be the root of the table name plus 'ID'. [Primary key for tblBoxes would be BoxesID].

Row GUID [if a GUID is required]

Should be the root of the table name plus 'GUID'. [Row GUID for tblCardboard would be CardboardGUID].

Description Field

Should be the root table name plus 'DESC'. [Description field for tblShipment would be ShipmentDESC].

Code Field (an abbreviated description for easy lookup)

Should be the root table name plus 'CODE'. [The code column for table tblState would be StateCODE].

Foreign Key

The foreign key field should be named identically to the primary key field in the originating table. [Foreign key of tblShipment in tblBoxes would be ShipmentID] Exception: when foreign key needs to be referenced more than once in a given table. In this case the Name should be a short description of why referenced plus the normal foreign key name. [if in tblShipment, tblState is referenced twice then something like this should be used ShipperStateID and ReceiverStateID]

Naming of Indexes

Primary Key:	PK_ColumnName
Non-Clustered Index:	NX_ColumnName
Clustered Index:	CX_ColumnName
Unique Constraint:	U_ColumnName
Unique Non-Clustered Index:	UNX_ColumnName
Unique Clustered Index:	UCX_ColumnName
Foreign Key:	FK_ColumnName_ColumnName

Best Practices

Whenever possible stored procedures should be used instead of ad hoc queries. Stored procedures have a filed execution plan, which allows for faster execution than an ad hoc query.
Triggers should be avoided in preference of stored procedures, which execute all update components and maintain referential integrity.
All tables should have an Identity column set on the primary key (integer or big integer [if more than 2 billion records are expected]) with a seed value of 1 and an increment of 1.
All tables in any database, which may need to be replicated, must have a unique key.
Whenever tables have a defined relationship that relationship should be enforced at the database level not only at the application level.
Security should be set to Mixed Mode [SQL Server and Windows NT], utilizing existing NT Group whenever possible.
All database objects should be created with 'dbo' as the owner. This will not happen automatically in our new development environment, so it should be specified during object creation.

Backup

All databases should be backed up to a remote device.
All production databases should have periodic transactional backup. Frequency to be determined by the number of transactions, and acceptable level of loss.
No production database should be set to 'Truncate on Checkpoint' in SQL 6.5, or Simple or Bulk-Logged Recovery Mode in 2000.
Remote backups should be maintained for critical information.

Maintenance

All databases should be reindexed regularly.
All databases should have regular DBCC checks performed to maintain integrity.
Indexes should be examined regularly to insure that they are optimal for performance.

Change Control and Documentation

All changes to a database should be documented and distributed to all concerned parties.
Major changes must be approved before implementation.
All procedures should have text describing use and purpose of each step in the process.

Security

All security should be maintained at the database level not the application level.
All modification to tables should be through stored procedures, not direct table updates. Whenever possible security should be implemented as access to stored procedures and views, not by granting access to the whole database.

Password Policy

Users are required to maintain strict password security. To facilitate this Computer Services has implemented the following password policies at the OS level.

Password Expiration

Passwords will be set to expire after 90 days of use.

Password Uniqueness

A given password cannot be reused until after 5 other passwords have been used.

Password Privacy

It is the responsibility of each user to maintain their own password privacy. A password should never be written or posted on the keyboard, monitor, or anywhere else in public view. A user should not give their password to any other user. A user should not allow another user to use a computer, which is logged on as them. A user should select passwords that will be difficult for another user to guess. Best practices suggest that passwords should not be the users name, the name of a child or close relative, a common word found in the dictionary, or an obvious date such as the users birthday. Best practices also suggest that a password consist of a combination of letters, numbers and special characters. For example, 'aardvark' would be a poor choice of passwords, where as 'Aardvark_89' would be much better.

Password Length and Complexity

A password must be a minimum of 8 characters. At this time we do not require the password to be complex (using numbers, special characters, and letters), but best practices suggest that users should attempt to choose secure passwords (see **Password Privacy** for more information).

Event Documentation

Change Control

Any planned network/ server/ application upgrade or down time for maintenance should be accompanied by a Change Control. The change control should contain detailed information about the process and the reasoning behind the change. The appropriate supervisor within any effected department and within Computer Services must approve all changes. The change control should include any related documentation used as reference. Change Controls must be filed according to the effected device in room 102.

Network Event Log

Minor network events may be documented using the Network Event Log rather than a change control. A minor event would be one with which there is little or no user interruption, and where no change to hardware or software is taking place (i.e. Rebooting a crashed server).

Backup Logs

Anytime a backup fails, the log for that job should be printed out. A supervisor should then review the log and sign off on that review.

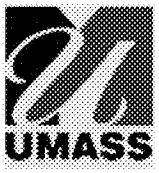
Outside Service Contractor

Anytime an outside vendor performs service on a server or network device a record of the service should be kept along with any other resulting documentation, as well as an explanation of why the service was performed. This should be filed by device in room 102.

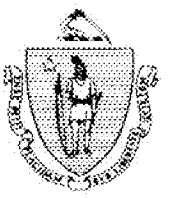
Appendices

Forms

Access Request Form



UMMS-JP AND DPH
EMPLOYEE ACCESS REQUEST FORM



This form is required for network and connectivity and security access. It must be completed **two weeks** in advance by the Supervisor/Manager of all new employees.

Section 1: User Information Check One: ___UMMS-JP ___DPH

First Name: _____ Middle Initial: _____ Last Name: _____

Phone Ext.: _____ Department: _____ Room #: _____

Supervisor/Manager: _____ Start Date: ____/____/____

User is a… (check one) ___Full-Time User ___Part-Time User ___Student/Temp

This request is for… (check one)
___Add new user ___Terminate user (see section 3 below) ___Modify user (see section 2 below)
(ie. User changes department)

Programs/Applications/Groups authorized to access or user with equivalent access: (indicate if this is an Addition [A] or Deletion [D])

1. _____ 4. _____
2. _____ 5. _____
3. _____ 6. _____

Section 2: Other Options

___Change User Name: From _____ To _____

___Reset password

___User Move or Relocation: From _____ To _____

Section 3: User Termination

Effective Date: ____/____/____

Resource Management

Personal Folder (F:\private\username\): (select one) ___Delete ___Backup then Delete
___Transfer files to _____

Email: (select one) ___Delete ___Backup then Delete
___Transfer EMail to User _____

Section 4: Email

Email Distribution Lists: (indicate if this is an Addition [A] or Deletion [D])

All users must be in one of the following:

_____ UMMS-JP (All Umass Non-Biologics Employees)
_____ BIO-JP (All Umass Biologics Employees)
_____ DPH-DL---SLI Staff (All DPH Employees)

Other Distribution Lists: (indicate if this is an Addition [A] or Deletion [D])

_____ _____ _____ _____

Section 5: Approval (every request must be authorized by a Supervisor/Manager)

Employee Signature: _____ Date: ____/____/____

Supervisor/Manager Signature: _____ Date: ____/____/____

Change Control Form

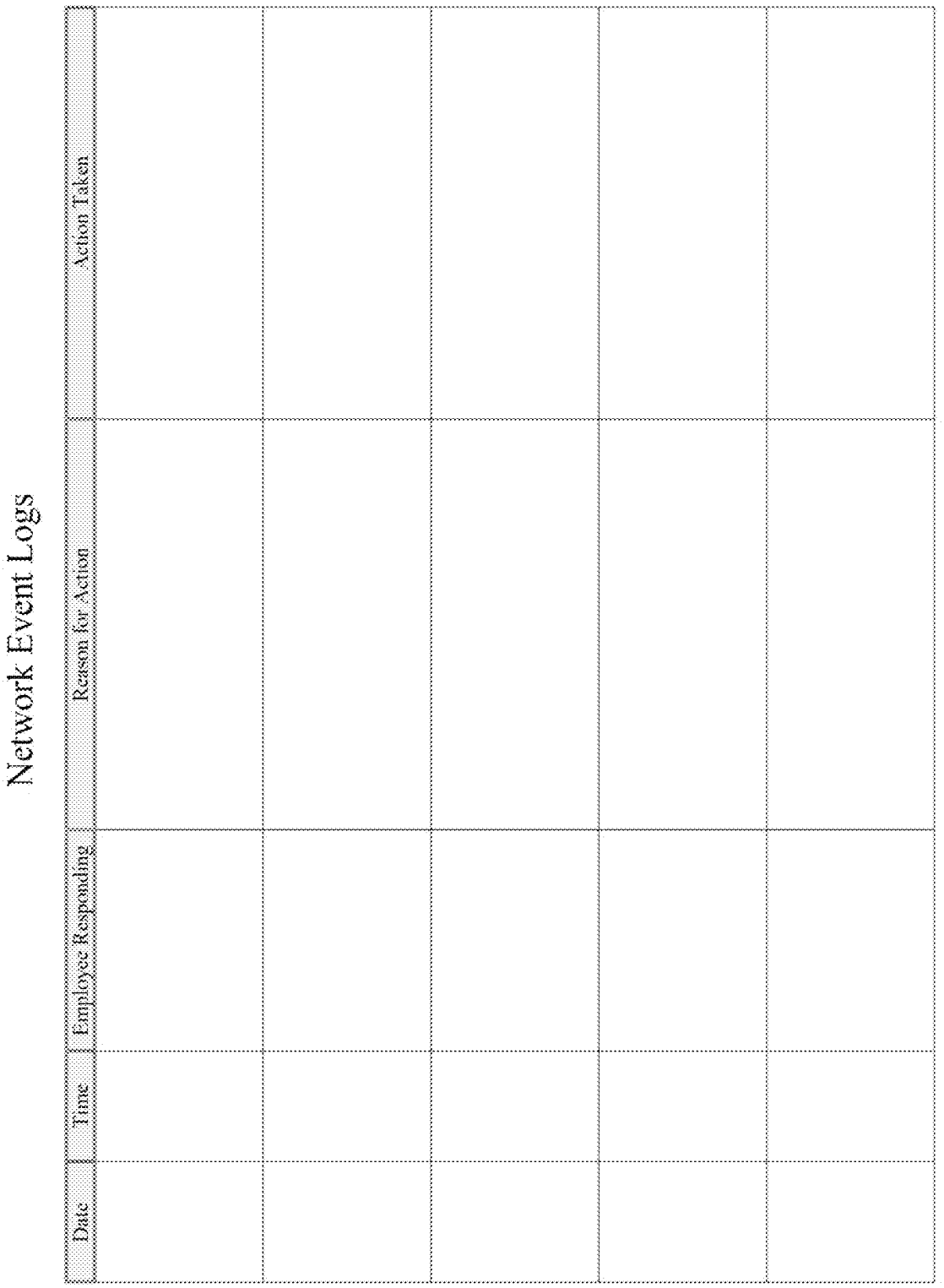
Medical School (Jamaica Plain)

Change Control Form

Project Name	
Date Submitted	
Submitted By	
Service Impact	
User Impact	
Detailed description	
Reason for Change (describe benefit)	
Date / Time Service Will Be Down	
Expected Downtime Length	
Date / Time Service Will Be Up	
Backout Time (how long to un-do)	
Date / Time User Message(s) Sent	

	Groups Impacted:	**Approving Authority:**	**Approved:**
	Desktop Services	Frank Christy	
	Data Center	Sean Fiandaca	
	Network & Systems	Kevin Gillespie	
	Newborn Screening	Mark Schwerzler	
	Biologics	John Fitzmaurice	
	SLIS	Patti Lautner	
	Final Approval:	Eric Solomont	

Network Event Log



CIM Test Form

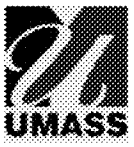
UMASS *Medical School (Jamaica Plain)*

Compaq Insight Manager Test Form

Test Performed	
Date Submitted	
Submitted By	
Detailed Description	
Expected Result	
Actual Result	

	Groups Impacted:	Approving Authority:	Approved:
	Systems Administrator	Sean Fiandaca	
	Network Administrator	Kevin Gillespie	
	CIM Project Manager	Arthur Benjamin	

Critical Contact List



Critical Contact List

Administration
Administration

Human Resources	Extension
Cormier, Carol	6206

Bureau of Communicable Diseases
Communicable Disease Control

Administration	Extension
Dooley, Jacqueline	6559

Bureau of Communicable Diseases
Epidemiology and Immunization

Epidemiology	Extension
McNamara, Ann	6235

Bureau of Communicable Diseases
Epidemiology and Immunization

Surveillance	Extension
Daniel, James	6808

Bureau of Communicable Diseases
HIV/AIDS Surveillance

HIV/AIDS Surveillance	Extension
Federico, Anne	6563

Bureau of Communicable Diseases
Refugee and Immigrant Health

Main Office	Extension
Cochran, Jennifer	6596

Bureau of Communicable Diseases
Sexually Transmitted Disease

Administration	Extension
Tang, Yuren	6554

Bureau of Communicable Diseases
Sexually Transmitted Disease

Main Office	Extension
Beck, Ann	6942

Bureau of Communicable Diseases
Tuberculosis Prevention and Control

Main Office	Extension
Shamprapai, Sharon	6958

2/1/2005 1

Critical Contact List

Bureau of Laboratory and Environmental Scien
Clinical Diagnostic Labs

Administration	Extension
Han, Linda	4362

Bureau of Laboratory and Environmental Scien
Clinical Diagnostic Labs

Bacteriology	Extension
Caloggero, Dina	6601

Bureau of Laboratory and Environmental Scien
Director's Office

Administration	Extension
Pribeck, Kristen	6212

Bureau of Laboratory and Environmental Scien
Director's Office

Training	Extension
Sullivan, Julie Schmitt	6255

Bureau of Laboratory and Environmental Scien
Environmental Labs

Blood Lead Lab	Extension
Rubin, Alan	6666
Jacobsen, Patricia	6668

Bureau of Laboratory and Environmental Scien
Environmental Labs

Environmental Lab	Extension
Nassif, Julianne	6651

Umass Medical School
Bio Labs

Administration	Extension
Fitzmaurice, John J	6688

Umass Medical School
Bio Labs

Engineering	Extension
McNeil, Greg	6446
Murphy, Peter	6480

Umass Medical School
Bio Labs

Technical Services	Extension
Canzano, Ami	6439

Critical Contact List

Umass Medical School
Computer Services

Computer Services	Extension
Fiandaca, Sean	6258
Solomont, Eric	6257

Umass Medical School
Facilties Department

Administration	Extension
Abbott, Brian	6545

Umass Medical School
Newborn Screening

Data Processing	Extension
Schwerzler, Mark	6335

Umass Medical School
Newborn Screening

Director's Office	Extension
Eaton, Roger, Dr	6317

2/1/2005 3

Illustrations

Illustration A

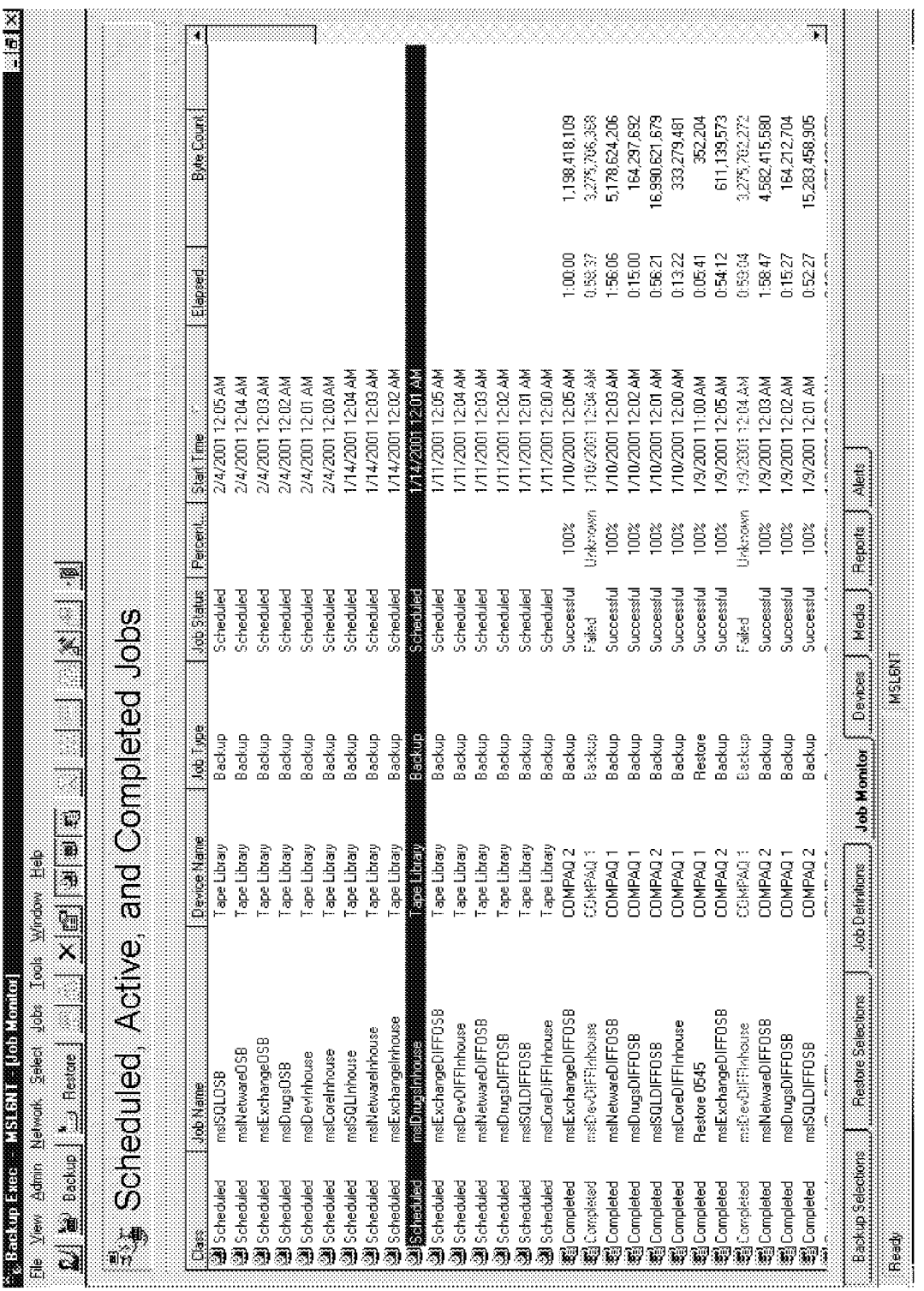


Illustration B

Name	Status	Notes	Date:12/16/02	Tape
NetwareINCosb	**S** / F			
DatabaseDIFFOSB	**S** / F			
mslDrugsDIFFOSB	**S** / F			
mslCoreDIFFInhouse	**S** / F			
mslDevDIFFInhouse	**S** / F			
Name	**Status**	**Notes**	**Date:12/17/02**	**Tape**
NetwareINCosb	S / F			
DatabaseDIFFOSB	S / F			
mslDrugsDIFFOSB	S / F			
mslCoreDIFFInhouse	S / F			
mslDevDIFFInhouse	S / F			
Name	**Status**	**Notes**	**Date:12/18/02**	**Tape**
NetwareINCosb	S / F			
DatabaseDIFFOSB	S / F			
mslDrugsDIFFOSB	S / F			
mslCoreDIFFInhouse	S / F			
mslDevDIFFInhouse	S / F			
Name	**Status**	**Notes**	**Date:12/19/02**	**Tape**
NetwareINCosb	S / F			
DatabaseDIFFOSB	S / F			
mslDrugsDIFFOSB	S / F			
mslCoreDIFFInhouse	S / F			
mslDevDIFFInhouse	S / F			
Name	**Status**	**Notes**	**Date:12/20/02**	**Tape**
NetwareINCosb	S / F			
DatabaseDIFFOSB	S / F			
mslDrugsDIFFOSB	S / F			
mslCoreDIFFInhouse	S / F			

Illustration C

First Sunday		**Notes**	**Date:12/01/02**	**Tape**
DatabaseOSB	S / F			
MSLDrugsOSB	S / F			
MSLCoreInhouse	S / F			
MSLDevInhouse	S / F			
LeadArchiveFullInhouse	S / F			
First Saturday				
Name		**Notes**	**Date:12/07/02**	**Tape**
NetwareFullOSB	S / F			
Third Saturday				
Name	**Status**	**Notes**	**Date:12/21/02**	**Tape**
NetwareFullOSB	S / F			

Illustration D

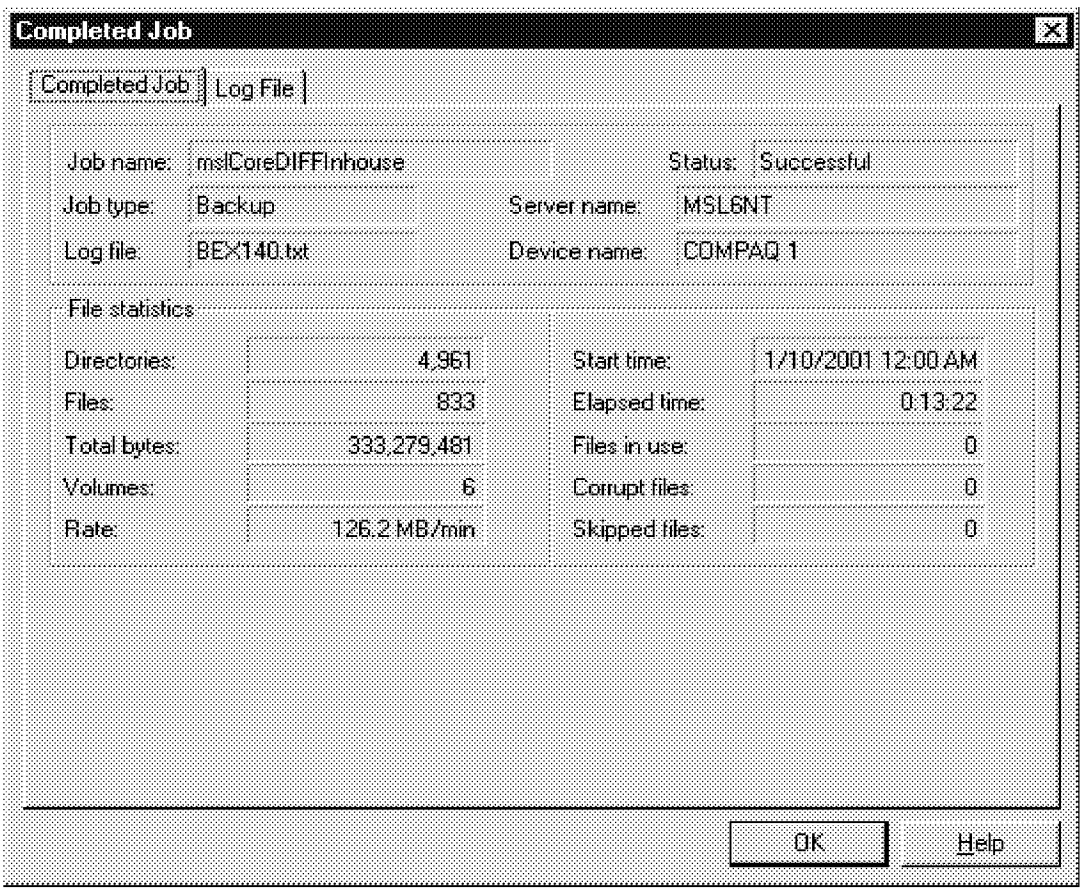


Illustration E

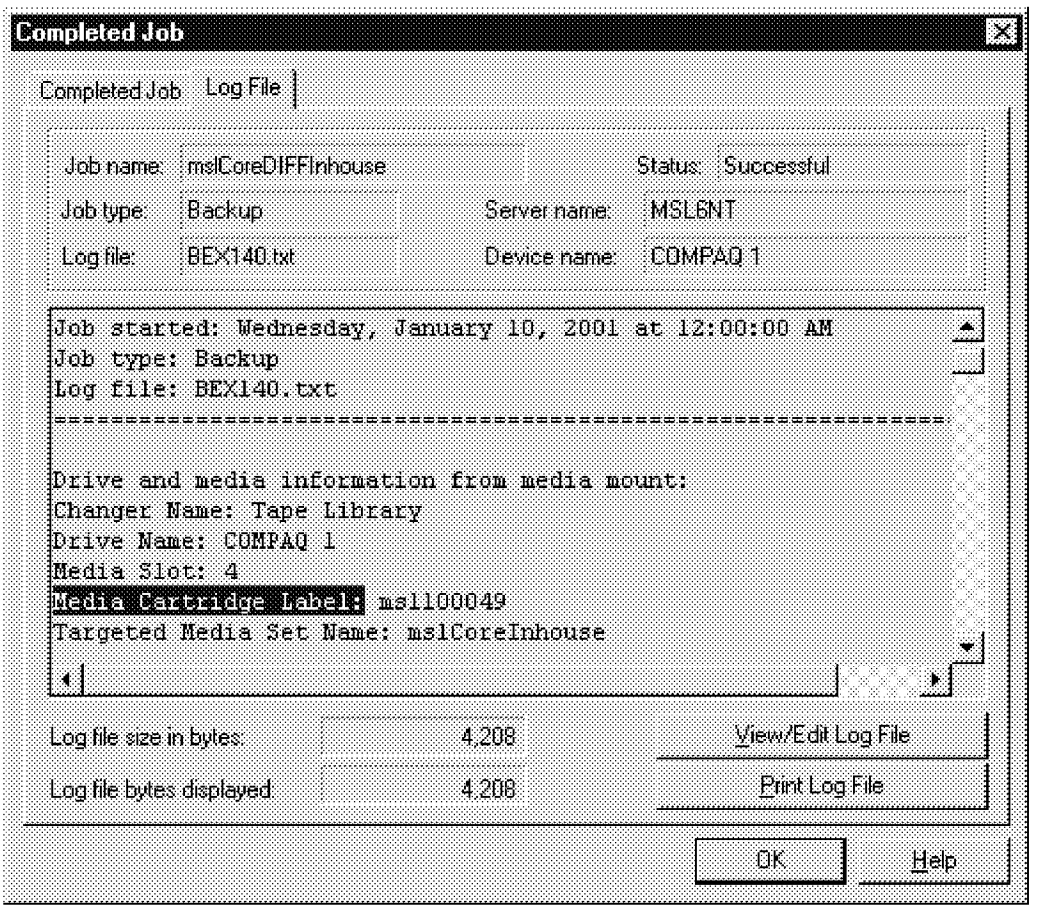


Illustration F

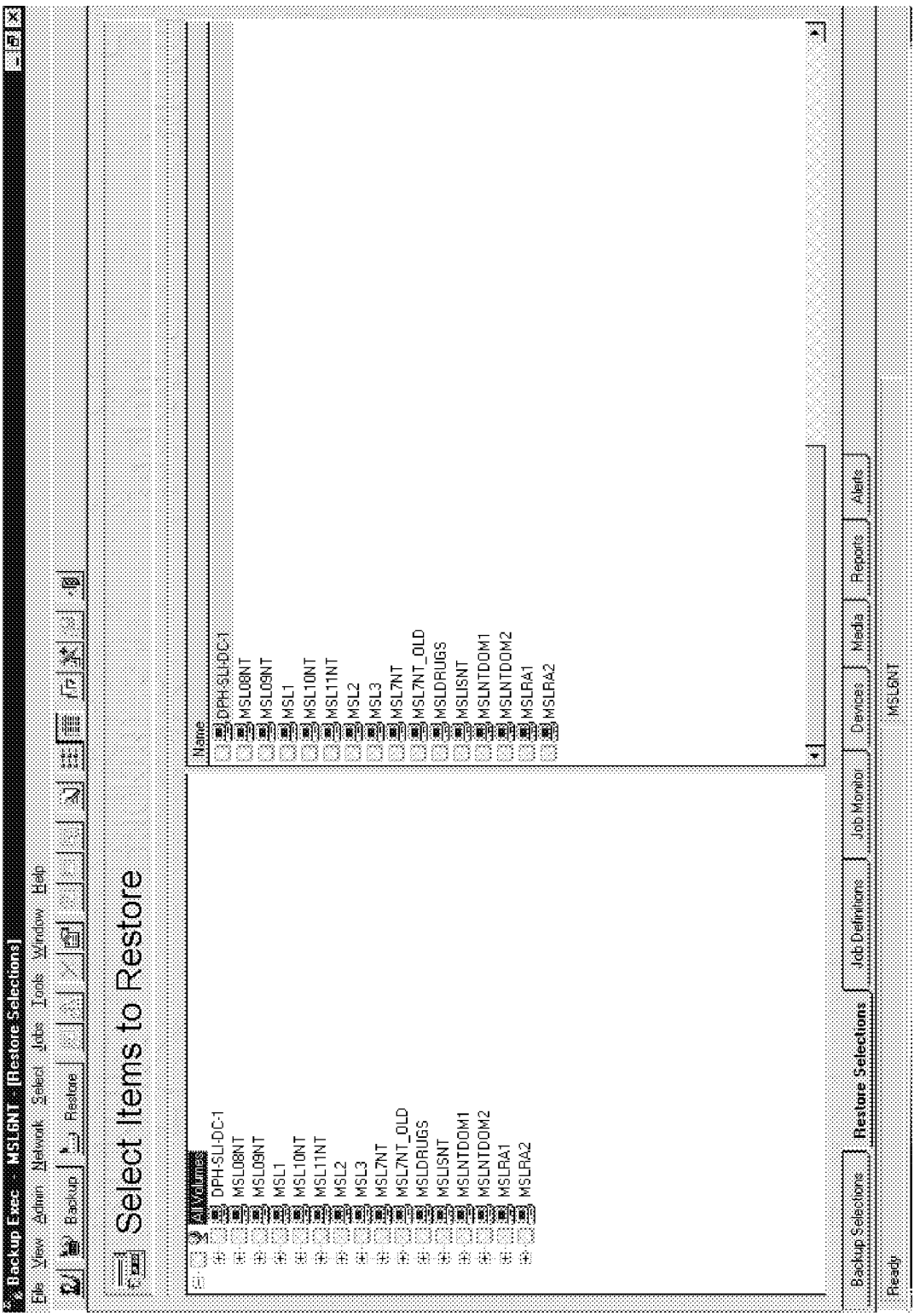


Illustration G

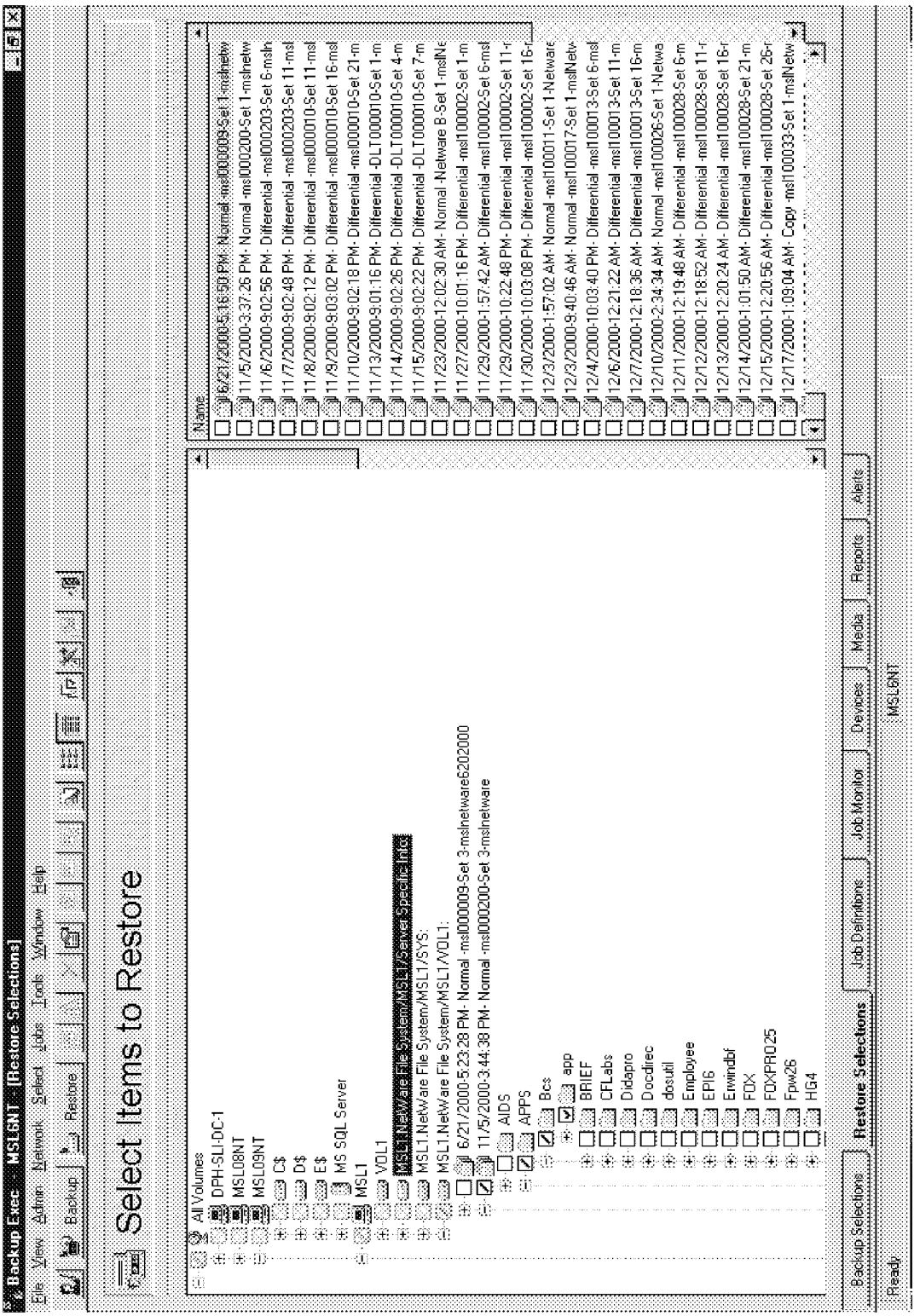


Illustration H

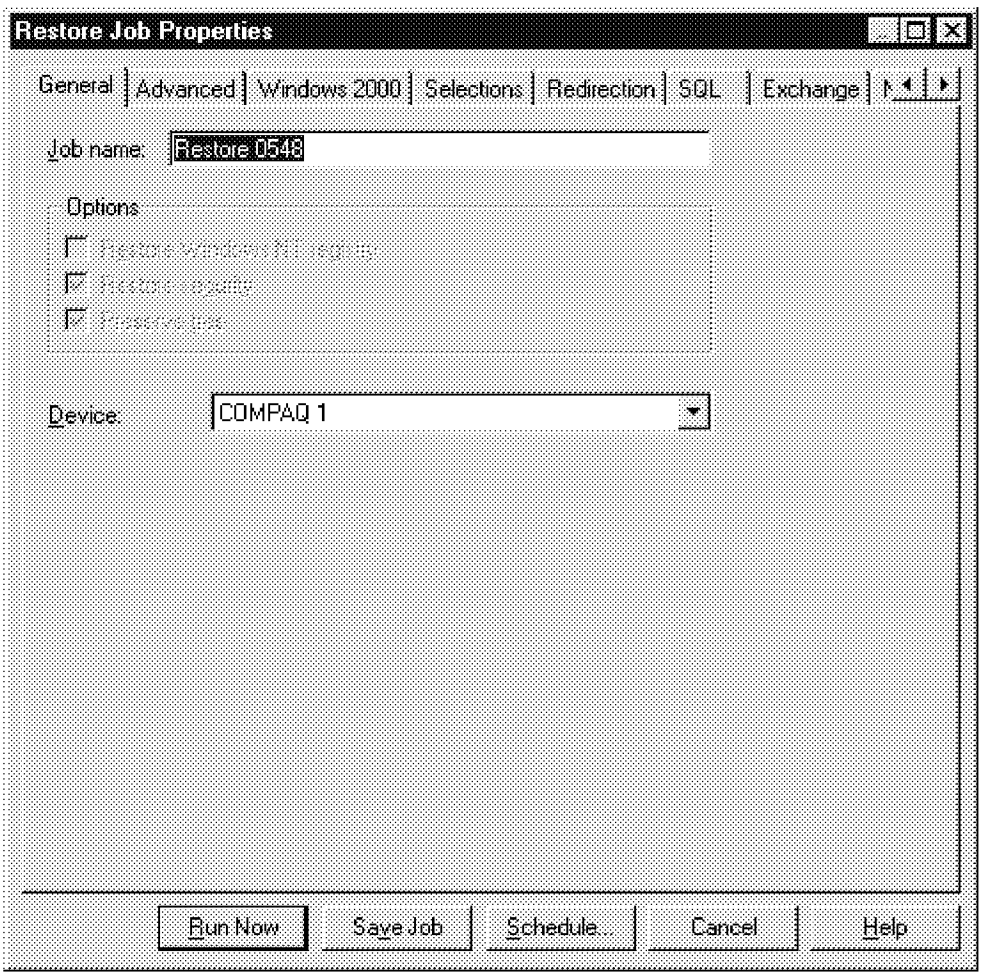


Illustration I

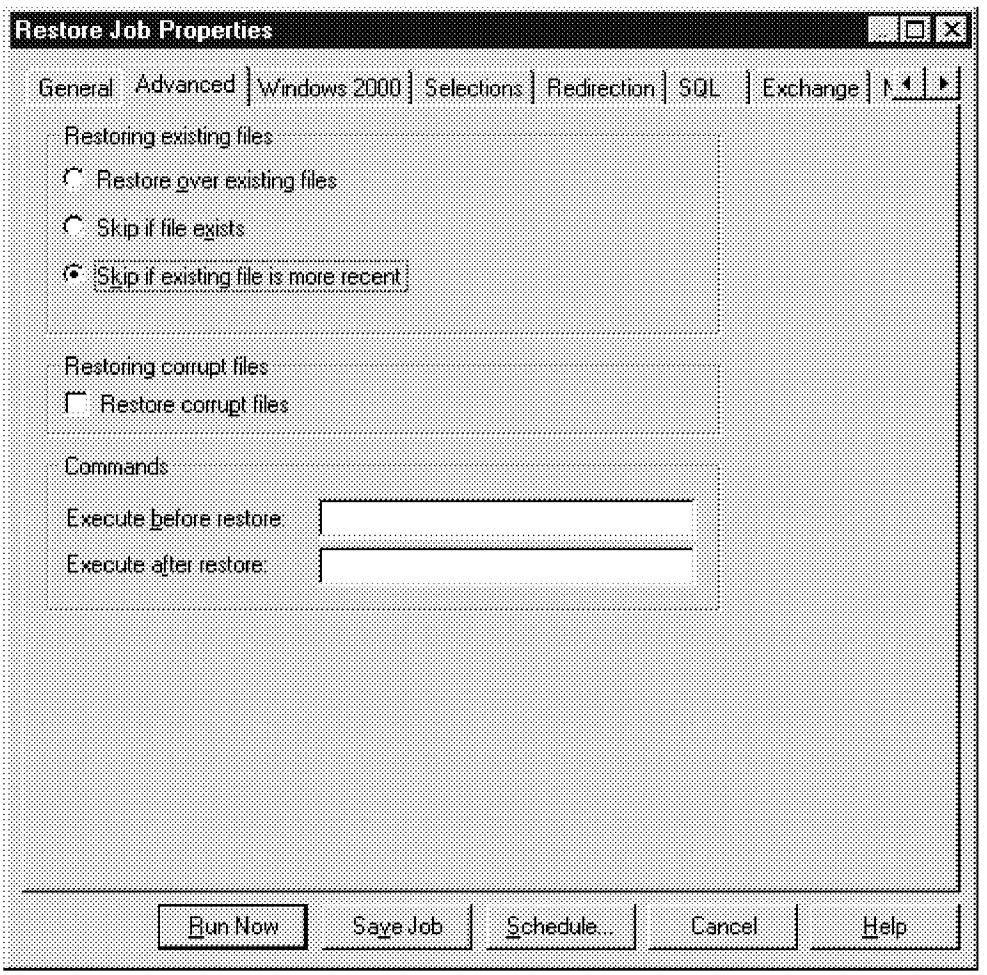


Illustration J

Name	Status	Notes	Date:12/09/02	Tape
PrivateIncINH	S / F			UM0016
SharedIncOSB	S / F			UM0010
BioServersIncOSB	S / F			UM0012
CoreIncINH	S / F			UM0017
ExchangeIncOSB	S / F			UM0013+0018
Name	**Status**	**Notes**	**Date:12/10/02**	**Tape**
PrivateIncINH	S / F			UM0016
SharedIncOSB	S / F			UM0010
BioServersIncOSB	S / F			UM0012
CoreIncINH	S / F			UM0017
ExchangeIncOSB	S / F			UM0018
Name	**Status**	**Notes**	**Date:12/11/02**	**Tape**
PrivateIncINH	S / F			UM0016
SharedIncOSB	S / F			UM0010
BioServersIncOSB	S / F			UM0012
CoreIncINH	S / F			UM0017
ExchangeIncOSB	S / F			UM0018
Name	**Status**	**Notes**	**Date:12/12/02**	**Tape**
PrivateIncINH	S / F			UM0016
SharedIncOSB	S / F			UM0010
BioServersIncOSB	S / F			UM0012
CoreIncINH	S / F			UM0017
ExchangeIncOSB	S / F			UM0018
Name	**Status**	**Notes**	**Date:12/13/02**	**Tape**
PrivateIncINH	S / F			
SharedIncOSB	S / F			
BioServersIncOSB	S / F			
CoreIncINH	S / F			
ExchangeIncOSB	S / F			

Illustration K

Backup Server EDJPBU01				
First Sunday Check List				
Name		**Notes**	**Date:1/5/03**	**Tape**
DatabaseFullOSB	S / F			
PrivateFullINH	S / F			
SharedFullOSB	S / F			
BioServersFullOSB	S / F			
CoreFullINH	S / F			
ExchangeFullOSB	S / F			
Second Sunday Check List				
Name	**Status**	**Notes**	**Date:1/12/03**	**Tape**
DatabaseFullOSB	S / F			
Third Sunday Check List				
Name	**Status**	**Notes**	**Date:1/19/03**	**Tape**
DatabaseFullOSB	S / F			
PrivateFullINH	S / F			
SharedFullOSB	S / F			
BioServersFullOSB	S / F			
CoreFullINH	S / F			
ExchangeFullOSB	S / F			
Fourth Sunday Check List				
Name	**Status**	**Notes**	**Date:1/26/03**	**Tape**
DatabaseFullOSB	S / F			
Fifth Sunday Check List				
Name	**Status**	**Notes**	**Date: N/A**	**Tape**
DatabaseFullOSB	S / F			

Approval Form

Document prepared by:

_____

Name Date

Document Reviewed By:

_____

Name Date

Scheduled For Next Review on:

_____

Date